Contents

1. Introduction

1.1 BT's customers have an expectation that BT and its 3rd Party supply chain provide their services using industry standard information security management systems (ISMS). The 3rd Party's ISMS should cover infrastructure, networks, equipment and IT systems in order to protect services being provided and BT/BT customer information in scope of the services. This document sets out BT's Security Requirements and applies to all 3rd parties working for or on behalf of BT Group, including Openreach, EE and Plusnet, here on referred to as 'BT' for the rest of the document. 3rd Party will be advised which security control sets are applicable to the service it is providing to BT.

1.2 These Security Requirements are in addition to and without prejudice to any other obligations of the 3rd Party in the Contract. They are designed to ensure that BT retains control and oversight of its network and user data.

2. Limited Access Requirements

2.1 Without prejudice to any obligations of confidentiality it may have, where 3rd Party Personnel have Access to BT Information, the 3rd Party must:

2.2 Ensure BT Information is not disclosed to or accessed by 3rd Party Personnel unless necessary for the provision of the Service; and

2.3 Put in place all systems and processes both technical and organisational as are required to protect BT Information (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or Access to BT Information in accordance with Good Industry Security Practices.

3. General Information Security

3.1 On reasonable request the 3rd Party shall make available to BT copies of security certifications and statement of compliance relevant to the Service to illustrate evidence of compliance with these Security Requirements.

3.2 Should there be a significant change to technology or industry security standards; or there are any material changes to the Services or how they are provided, BT may issue a Contract amendment during the term, if there is a need for a change to the applicable security control sets. The 3rd Party shall comply with the agreed Contract amendment within a reasonable time considering the nature of change and the risk to BT.

3.3 When there are any material changes to the Services or how they are provided, 3rd Party must review this Security Requirements policy to ensure they are still compliant to all applicable security controls.

3.4 If the 3rd Party subcontracts obligations under the Contract, then the 3rd Party shall ensure all Contracts with relevant Subcontractors and their Subcontractors, include written terms requiring the Subcontractor to comply with the applicable parts of either these Security Requirements or to equivalent 3rd Party security requirements.

3.5 If a 4th party will be used to provide the service, where they will hold or process BT Information, the 3rd Party must obtain agreement from the BT Stakeholder what information can be shared. The 3rd Party must ensure they have a contractual

relationship with the 4th party and must ensure the 4th party operates an industry standard security framework.

3.6 BT Information may be retained for as long as necessary to perform the Contract, after which it should be retained no longer than a maximum of two years, unless a different retention period has been agreed between BT and 3rd Party or is required by any applicable laws.

3.7 If the Services are in direct support of a UK Government Contract, the 3rd Party must comply with the most current version of the Cyber Essentials Plus - https://www.cyberessentials.ncsc.gov.uk/

3.8 Where BT Information will be processed or stored offshore 3rd Party must advise BT of the geographical locations, BT reserves the right to reject locations that are deemed high risk.

Handling BT Information

3.9 Unless advised otherwise by the BT stakeholder all BT Information is classified as "Confidential". Where personal data or sensitive personal data is in scope advice should be sought from 3rd Party's Data Protection and Privacy Team in case additional controls are required.

The following security controls are "voice handling requirements" which have a scope limited to verbal communications.

3.10 If there is a need to discuss, show or exchange BT Information using a collaboration platform (e.g. Teams)

- Ensure only individuals who have a need to know the information are present.
- If there is an external contractor involved, they must have either a signed contract with the 3rd Party or have an NDA in place prior to discussions starting.
- 3rd Party must verify who is on the conference before starting.

3.11 If there is a need to discuss BT Information with someone face to face, on a mobile phone or standard telephone line.

- Conversations must not be held or overheard by anyone who does not have a need to know.
- If the conversation is required with an external contractor, they must have a signed contract with 3rd Party, or an NDA must be in place prior to discussions starting.
- Confidential or Highly Confidential information must not be left on voice mail services.

The following security controls are "written handling requirements" and have a scope covering material kept in paper format. This includes but is not limited to handwritten letters, minutes, notes, and memos. It also includes printed electronic material such as work documents and reports once they are in a paper format.

3.12 If storing paper copies of BT Information at 3rd Party premises, when not in use these must be secured in a lockable facility, with access restricted to only those with a need to view the material. Documents must not be left unattended.

3.13 If there is a need to print, photocopy or duplicate BT Information, the following security controls apply:

- Only use the printing or copying facilities at 3rd Party's own premises.
- Photocopies or printouts must not be left unattended at the print location and must be collected at the time of creation.
- Where the printer or photocopier has memory capability where copied material can be recalled and re-printed this should be restarted to clear memory as soon as practicable.

3.14 If there is a need to remove copies of BT Information from 3rd Party premises:

- Unless already agreed as part of the scope of work 3rd Party must obtain evidenced consent from the BT stakeholder.
- If approved, the information must not be identifiable whilst in transit and must held in an anonymised or plain folder, bag, or case.
- The material must not be left unattended and must remain in the direct control of the person transporting the material, especially on public transport.

3.15 When no longer required paper copies of BT Information must be disposed of as follows:

- Paper copies must not be disposed of in the general waste bins.
- If using a shredder, it must be a minimum standard of P4 DIN66399.
- If approved shredders are not available information must be disposed of in confidential waste bins.

For "Highly Confidential information" the following additionally applies:

- Information must only be disposed of in confidential waste bins after being shredded.
- Information that is required to be shredded on site by the supplier, must gain a certificate of destruction from the supplier.

The following security controls relate to BT Information in electronic format.

3.16 When storing BT Information on 3rd Party PC or Laptop the following controls apply:

- Only allowed on devices with hard disk encryption (e.g. Bitlocker).
- All documents must be individually encrypted.
- Information Rights Management (IRM) must be applied to the document.
- If supplied, information must retain the BT classification label.

3.17 When saving a BT document to an internal file sharing location for general storage, collaboration or file sharing; the following security controls apply:

- The location the material is being stored to must have access permissions applied to only allow those with a need to see or use the document.
- If supplied, information must retain the BT classification label.
- All documents must be individually encrypted.

- Information Rights Management (IRM) must be applied to the document.
- If in scope of the service being provided PCI and Payment card material must not be saved to file storage sites at any time.
- If guest accounts are required to provide access to an external contractor they must have a signed contract with 3rd Party or an NDA must be in place prior to access being granted.

3.18 If there is a need to save BT Information on 3rd Party removable media (e.g. a USB memory stick) the following security controls apply:

- The device must be encrypted to the same level as the hard drive.
- If lost or stolen 3rd Party must raise a security incident.
- 3rd Party must have the evidences of prior approval from the BT Stakeholder to transfer "highly confidential" material to removable media.
- If in scope of the service, PCI material or personal data must not be stored on removable media.
- Devices intended for support and maintenance shall not be used for any other purpose.

3.19 BT Information must not be stored on personal PC's, laptops, removable media or mobile devices

3.20 BT Information must not be sent or auto-forwarded from a 3rd Party corporate email address to a personal e-mail or external email account unless they are an external contractor that has a signed contract with 3rd Party or an NDA in place and is used to provide the service.

3.21 To minimise the attack surface and the opportunities for attackers to manipulate human behaviour though their interaction with web browsers and email systems, implement processes to ensure that only fully supported web browsers and email clients are allowed and uninstall or disable any unauthorised browser or email client plugins or add-on applications.

3.22 3rd Party must have back-up measures in place in order to restore BT Information within 3 working days, in the event of corruption, loss or degradation.

3.23 When disposing of BT data/Information, full records of data retention and disposal must be kept, providing audit trail, evidence and tracking. This must include:

- Proof of destruction and/or disposal (including date undertaken and method used).
- System audit logs for deletion.
- Data disposal certificates.
- Who undertook the disposal (including any disposal partners / 3rd parties or contractors).
- A destruction and verification report must be generated to confirm the success or failure of any destruction / deletion process. (i.e. an overwriting process must provide a report that details any sectors that couldn't be erased).

3.24 When disposing of equipment where BT data/information was present, an audit trail must be provided for the following equipment types:

- Removable media.

- Disk Drives.
- Back-up tapes.
- Computer components.

3.25 Full records must exist to provide an audit trail to include as a minimum:

- The name of the application or service that utilised this piece of equipment.
- Equipment type e.g. desktop, laptop, server, tape, router etc.
- Number of hard drives the equipment contains (if applicable).
- Equipment identified by serial number.
- Component parts of equipment identified by serial number.
- Full asset tracking of all equipment and component parts through the entire equipment disposal lifecycle.
- Proof of destruction and/or disposal (including date undertaken and method used).
- Details of who undertook the disposal (including any disposal partners / 3rd parties / waste disposal contractors).
- A destruction and verification report must be generated that confirms the success or failure of any recycling/sanitisation or destruction process. For example, an overwriting process must provide a report that details any sectors that couldn't be erased. These reports should include the capacity, make, model and serial number of the media.

Roles & Responsibilities

3.26 Every 3rd Party must be aware and understand the requirements of these security controls and are responsible for making sure that all individuals who are involved in providing a service to BT are familiar and comply with the relevant requirements of this standard.

Governance

3.27 The 3rd Party must have an established and consistent industry standard security framework for information and cyber security governance which covers the following components:

- Appropriate Information and Cyber Security policies and procedures which are approved and communicated.
- An information security strategy.
- Relevant legal and regulatory requirements regarding Information and Cyber Security (including privacy) which are understood and managed.
- Governance and risk management processes which address information and cyber security risks.

3.28 The 3rd Party must ensure that appropriate roles and responsibilities for Information and Cyber Security defined and implemented which includes the following:

- A full-time Chief Information Security Officer (or equivalent) who is sufficiently senior and has responsibility for information security programme.
- A high-level working group, committee or equivalent body which coordinates information security activity across the 3rd Party which is chaired by a suitably senior member of staff and meets on a regular basis.
- A specialist information security function with suitable and defined roles and responsibilities.

3.29 The 3rd Party must ensure that there is individual accountability for information and systems by ensuring that there is appropriate ownership of critical business environments, information, and systems and that this is assigned to capable individuals.

3.30 The 3rd Party must ensure that BT is notified (in writing) as soon as they are legally able to do so if the 3rd Party is subject to a merger, acquisition, or any other change of ownership.

Incident Management

3.31 The 3rd Party must have an established and consistent incident management framework to ensure that incidents are appropriately managed, contained and mitigated and covers the following components:

- Ensuring that personnel know their roles and order of operations when a response is needed.
- Ensuring incidents reported consistent with established criteria.
- Ensuring that the impact of the incident is understood.
- Ensuring that forensics are performed where necessary either internally or by a specialist function.
- Ensuring that lessons learned from incidents are incorporated into best practice.
- Ensuring information related to an incident impacting BT is treated as "Confidential".

3.32 The 3rd Party will take all reasonable steps to ensure appropriate individual(s) are appointed and made responsible as Point of Contact for security risk, incident management and compliance management. 3rd Party shall notify BT Stakeholder of the individual(s) contact details and any change to them.

3.33 The 3rd Party will inform BT via email security@bt.com or by telephone 0800 321 999, within a reasonable timeframe upon becoming aware of any incident that impacts the service to BT or BT Information, and in any event, no later than twenty-four (24) hours from the time the Incident comes to 3rd Party's attention.

3.34 The 3rd Party without unreasonable delay, will take appropriate and timely corrective action to mitigate any risks and effects related to the incident to reduce the severity and duration of the incident.

3.35 The 3rd Party will provide within 30 days of an incident a report to the BT Stakeholder in respect of any incident that impacts the service to BT or BT Information, it should include as a minimum:

date and time, location, type of incident, impact, status, and outcome (including the resolution recommendations or actions taken).

3.36 The 3rd Party must perform a root-cause analysis of all security incidents. Outcomes of this analysis should be escalated to the appropriate management level within the 3rd Party's organisation.

Change Management

3.37 The 3rd Party must ensure that all IT changes are approved, logged, and tested, including backing out of failed changes, prior to implementation to prevent service disruption or security breaches and that there is a process for undertaking emergency updates in a controlled manner.

3.38 The 3rd Party must ensure that changes are reflected in both Production and DR environments.

3.39 The 3rd Party must ensure that maintenance and repair of organisational assets is performed and logged, with approved and controlled tools.

3.40 The 3rd Party must ensure that remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access.

Cyber Risk and Threat Management

3.41 The 3rd Party must ensure that there is an ongoing Cyber Security risk and threat assessment framework to ensure that the Cyber Security risk profile to the organisation's operations, assets, premises, and individuals is understood and managed by:

- Assessing asset vulnerabilities.
- Identifying both internal and external threats.
- Sensitivity of information / data in scope.
- Assessing potential business impacts.
- Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
- Ensuring that the Cyber risk and threat management framework is agreed at a suitable level in the organisation.

3.42 The 3rd Party must ensure that all risks and threats identified as part of the Cyber Security Risk and threat assessment are prioritised and action taken accordingly to mitigate the risks in a suitable timescale.

3.43 The 3rd Party must notify BT Stakeholder if they are unable to remediate or reduce any material areas of risk that could impact the service being provided.

Identity Management and Access Control

3.44 The 3rd Party must have an established and consistent framework to ensure that identities and credentials are managed securely by authorised personnel:

- Only granting, re-enabling, changing, and disabling of access rights based on documented and authorised approvals.
- Ensuring that dormant accounts are disabled.
- Disabling accounts of personnel who are no longer in employment.

- Implement processes and tools to track, control, prevent and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- Periodic reviews of access are in place to ensure that access is fit for purpose.
- User accounts have access recertified on at least an annual basis and privileged accounts have access recertified quarterly.
- Ensure persistent credentials and secrets (e.g., for break glass access) are protected within hardware-protected storage and are only made available to the responsible person(s) in an emergency.
- Ensure non-persistent credentials (e.g. username and password authentication) are stored in a centralised service with appropriate role-based access control which shall be updated in line with any relevant changes to roles and responsibilities within the organisation.

3.45 Central storage for persistent credentials shall be protected by hardware means. For example, on a physical host the drive could be encrypted with the use of a Trusted Platform Module (TPM). Where a virtual machine (VM) is used to provide a central storage service, that VM and the data included in it shall also be encrypted, use secure boot and be configured to ensure that it can only be booted within an appropriate environment. The 3rd Party must ensure that remote access is managed so that only approved individuals can connect remotely to the 3rd Party's Systems and that connections are secure and prevent data leakage and appropriate access control is in place such as multi-factor authentication.

Two factor authentication should be achieved with a User ID, Password and one of the following methods:

- A one-time password generator: that requires a user specific PIN/password to view the one-time password.
- A smart card with an ISO 7816-compliant chip and associated card reader and software. Contactless smart cards are not permitted.
- Certificate based authentication issued in accordance with the 3rd Party's Infosec certificate policy.

For avoidance of doubt if privileged access for support is provided via remote access, then this must be via a secure connection and use two factor authentication.

3.46 The 3rd Party must ensure that access permissions and authorisations for all systems (including tools, applications, databases, operating systems, hardware etc.) are managed incorporating the principles of least privilege and separation of duties.

3.47 The 3rd Party must ensure that each transaction can be attributed to a unique identifiable individual, and if there are any shared credentials that there are appropriate compensating controls (including break glass procedures). Shared credentials for privileged access are not permitted.

3.48 The 3rd Party must ensure that all authentication is managed commensurate with the risk of the transaction, i.e., appropriate password length and complexity, frequency of changes of passwords, multi-factor authentication, secure management of password credentials or other controls. Privileged access must be via accounts secured with multi-

factor authentication. 'Break-glass' privileged user accounts must have strong credentials unique to each network equipment point of access.

3.49 Appropriate controls must be in place to handle failed authentications, including screen notifications, logging of failure and user lockout.

3.50 Processes and controls must be in place to manage and authorise guest and service accounts.

Data Classification and Protection

3.51 The 3rd Party must have an established and consistent information classification, labelling and handling framework / scheme (aligned to Good Industry Practice / BT requirements) which contains the following components:

- Information handling guidelines.
- Information is protected in line with its assigned level of classification.
- Ensuring that all staff aware that BT Information shall not be used for any purpose other than that for which it was provided.

Data Leakage Prevention

3.52 The 3rd Party must have an established and consistent framework to ensure that protection against inappropriate data leakage is in place ensuring protection includes (but not limited to) the following vectors:

- Email, Internet / Web Gateway (including online storage and webmail), USB, Optical and other forms of ports / portable storage etc, Mobile Computing and BYOD, Remote Access Services, file sharing mechanisms and social media.
- Unauthorised devices must not be connected to the network (either the vendor's corporate network or BT's systems / network) or used to access non-public information.

Vulnerability Management.

3.53 The 3rd Party must have an established and consistent vulnerability management framework which includes the following components:

- Processes policies and procedures.
- Defined roles and responsibilities.
- Appropriate tools such as Intrusion Detection Systems and vulnerability scanning systems.

3.54 The 3rd Party's vulnerability management framework must ensure that the following are routinely monitored to detect potential cyber security events:

- Key systems and assets.
- Unauthorised connections.
- Unauthorised software / applications.
- Network activity.

3.55 The 3rd Party's vulnerability management framework must ensure that:

- There are processes established to receive, analyse, and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g., internal testing, security bulletins, or security researchers).
- Only authorised tools, technologies, users are permitted.
- Identified vulnerabilities are mitigated or documented as accepted risks.

Security Continuous Logging and Monitoring.

3.56 The 3rd Party must ensure that there is an established and consistent audit and log management framework which ensures that key systems including applications are set to log key events (including those of privileged access and personnel activity) with such logs being retained for a minimum period of 13 months. Logs for network equipment in Security Critical Functions must be fully recorded and made available for audit for 13 months.

As a minimum the 3rd Party must ensure that logs address the following events:

- System start-up and shutdown.
- Successful and unsuccessful authentication
- System log-on log-off
- Creation, modification, and deletion to/of accounts
- Credential change
- Privilege escalation
- Account lockout
- Hardware attachments and removals
- System and network management alerts and error messages
- Security event admin changes; including group management and security policy changes
- Start and stop points of the logged process
- Log activation or deactivation events
- Changes to the type of logged events as required by the audit trail (for example the start-up parameters and any changes to them).
- Log modification (or attempted modification)
- Any form of access to the management plane of systems used in connection with a UK public electronic communications network or service

As a minimum the 3rd Party must ensure that the following log parameters are captured for each event:

- Identity of asset to which the event relates
- Type of event
- Date and time of event
- An indication of success/failure of event
- Account user ID

- Identification of the source of event such as user/systems location, IP addresses terminal ID, terminal ID or other means of identification

3.57 The 3rd Party auditing, logging and monitoring framework must include the following components:

- Event logs generate alerts in real or near-real time to identify unauthorised activity
- Events and alerts are monitored by an independent function on a continuous basis and are investigated, triaged and assigned a level of severity
- Triaged alerts invoke Security Incident Management processes based on established protective monitoring use cases and playbooks in accordance with service level agreements and severity
- Logs are treated as having an information classification of "Confidential" as a minimum and protected against tampering, unauthorised access and loss
- Logging and monitoring activity is synchronised to an approved NTP time source
- Processes are established to identify and configure additional protective monitoring use cases and associated event logs, correlations and alerts necessary to address existing or emerging significant threats and risks

4. 3rd Party Personnel Security

4.1 The 3rd Party shall ensure that all 3rd Party Personnel have confidentiality agreements in place before any 3rd Party Personnel start working in BT buildings or on BT Systems or have Access to BT Information. These confidentiality agreements must be retained by 3rd Party and evidence be made available for audit by BT.

4.2 The 3rd Party shall deal with breaches of 3rd Party and applicable BT security controls and standards, through formal processes including disciplinary action which may include removal of the individual from:

- having Access to BT Systems or BT Information; or
- carrying out work connected with the provision of the Service.

In addition, the 3rd Party shall ensure they have relevant processes in place to ensure any 3rd Party Personnel who have been so removed are not subsequently given Access to BT Systems, BT Information or allowed to work in connection with the provision of the Service.

4.3 The 3rd Party shall, to the extent permissible by the law, maintain a confidential facility, to be used by the 3rd Party Personnel to anonymously report if they are instructed to act in a manner inconsistent or in violation of these Security Requirements. Relevant reports are to be notified to BT.

4.4 When 3rd Party Personnel are no longer assigned to the Service, at BT's option, any BT physical assets or BT Information in the possession of 3rd Party Personnel shall be either: handed back to the relevant BT operational team or securely destroyed as per security controls 3.22 and 3.23.

4.5 The 3rd Party must have an established and consistent framework on acceptable use of personal and corporate social media including ensuring personnel:

- do not post anything libellous, obscene, or abusive about the organisation, its clients or customers.
- do not use organisation or client logos without prior permission.
- do not expose organisation or client non-public information without prior consent.
- do not post opinions about the organisation its clients or customers which could reasonably be construed as official comment of the organisation or its clients.
- do not release any BT Information that is marked as 'General', 'Confidential' or 'Highly Confidential'.

4.6 The 3rd Party must ensure that all 3rd Party Personnel under their control undertake mandatory security of information training, which includes Cyber Security best practice and protection of personal data within one month of joining and refreshed at least on an annual basis including where appropriate:

- Privileged users
- 3rd Party stakeholders (e.g. Sub-contractors, customers, partners)
- Senior executives
- Physical and Cyber Security personnel

4.7 The 3rd Party must ensure that there is a testing component to verify that the user understands the training and awareness.

5. Audit & Security Review

5.1 Without prejudice to any other right of audit that BT may have, to assess the 3rd Party's compliance to the security controls in this Security Requirements policy, the 3rd Party will provide BT, or its representatives, access, and assistance as necessary and appropriate to allow document-based security reviews or on-site audits to be undertaken. A minimum of 30 working days' notice will be provided to 3rd Party prior to a routine onsite audit.

The scope of the audit will be to review any or all aspects of the 3rd Party's policies, processes, and system(s) (subject to the 3rd Party protecting the confidentiality of any information not related to the provision of the Service to BT), that are relevant to the Service being provided.

5.2 The 3rd Party will work with BT to implement agreed recommendations and carry out any corrective actions identified as necessary resulting from a document-based security review or on-site audit within 30 days of being notified by BT of a major non-compliance, 90 days of being notified by BT of a minor non-compliance, or such period as agreed between the parties at the 3rd Party's expense.

6. Right of Inspection

6.1 The 3rd Party must permit BT to undertake an inspection of the control environment where the services are developed, manufactured, or provided to perform security

compliance testing and/or assessments on reasonable request (or immediately following an incident).

6.2 The 3rd Party is responsible for the costs of remediating any security weaknesses identified by BT within a timescale as agreed by both Parties.

6.3 In the event of a serious incident the 3rd Party shall fully cooperate with BT in any ensuing investigation by BT, a regulatory authority and/or any law enforcement agency by providing access and assistance as necessary and appropriate to investigate the incident. BT may have need to request the 3rd Party quarantine for evaluation any relevant asset belonging to 3rd Party to aid the investigation and 3rd Party shall not unreasonably withhold or delay such request.

7. Security Certifications

7.1 The 3rd Party Systems, Service, associated Services, processes, and physical locations must be compliant with and shall continuously comply with the ISO/IEC 27001 standard (or certification(s) that demonstrate equivalent controls, supported by an independent auditor report) and any amended or future version of the standard issued. This compliance must be assured by certification of the 3rd Party's ISMS by a UK Accreditation Service (UKAS) or an international equivalent approved certification body where the scope and statement of applicability encompasses the services being provided at the locations they will be provided from.

7.2 The 3rd Party must submit a valid certificate at the start of the contract and on future re-certifications.

7.3 Should the scope of the certificate or statement of applicability be changed during the term of the contract to the extent it no longer covers all the services being provided at the locations they are provided from, the 3rd Party must advise BT within a reasonable time frame. The 3rd Party must inform BT within 2 working days of any major non-conformance identified by the certification body or the 3rd Party, which poses a risk to the services being provided.

8. Physical Security – BT Premises

8.1 The 3rd Party shall adhere to all relevant instructions provided to them with regards to access to BT premises and building entry systems. All 3rd Party Personnel working on BT premises shall be in possession of, and display prominently, a 3rd Party or BT provided identification card which must include a photographic image displayed on the card that is a clear and true likeness of the 3rd Party Personnel.

8.2 BT may also provide 3rd Party Personnel with an electronic access card and/or limited duration visitor card which shall be used in accordance with local issuance and revocation instructions

8.3 The 3rd Party is responsible for advising BT with 24 hours when a 3rd Party individual no longer requires BT building access and/or access to BT entry systems.

8.4 Only approved BT build servers, BT Webtop PCs and Trusted End Devices can directly connect (plug into LAN port or Wireless connection) to BT domains. The 3rd Party must not without the prior written authorisation from BT connect any equipment not approved by BT to any BT Domain.

8.5 Physical protection and guidelines for working in BT premises shall be adhered to, and shall include but not be limited to, the escorting of 3rd Party Personnel and the adoption of appropriate working practices within secure areas.

8.6 Where the 3rd Party is authorised to provide its 3rd Party Personnel with un-hosted access to areas within the BT estate; the 3rd Party authorised signatory and 3rd Party Personnel must adhere to the guidance document Supplier Access to BT's sites - Mandatory Security Guide Selling to BT.

9. Physical Security – 3rd Party Premises

9.1 The 3rd Party must have a physical access process that covers access methods and authorisation to 3rd Party premises (sites, buildings, or internal areas) where services are provided, or where BT Information is stored or processed. Access method shall include 1 or more of the following:

- An authorised 3rd Party identification card with a photographic image displayed on the card that is a clear and be a true likeness of the individual.
- An authorised electronic access card to access the applicable areas of the premises.
- Keypad security access, which must have processes for: authorisation, the dissemination of code changes (which must occur monthly, as a minimum); and ad-hoc code changes.
- Biometric recognition.

9.2 The 3rd Party must have processes and procedures for the control and monitoring of visitors and other external persons, including personnel with physical access to secure areas or for the purpose of environmental control maintenance, alarm maintenance and cleaning.

9.3 Secure areas in 3rd Party premises used to provide the service (e.g., network communications rooms) shall be segregated from general access areas and protected by appropriate entry controls to ensure that only authorised individuals are allowed access. Access made to these areas must be audited regularly and an assessment of re-authorisation of access rights to these areas must be carried out annually as a minimum.

9.4 The 3rd Party shall have CCTV security systems in locations where BT Information is stored or handled. Recordings and recorders must be securely located to prevent modification, deletion or the 'casual' viewing of any associated CCTV screens and access to the recordings must be controlled and restricted to authorised individuals only. CCTV recordings must be retained for a minimum of 20 days.

9.5 The 3rd Party must have implemented appropriate measures to ensure physical security with respect to the following:

- Fire prevention measures including but not limited to alarms, detection, and suppression equipment.
- Climatic conditions, with consideration given to temperature, humidity and static electricity and the associated management, monitoring, and response to extreme conditions (such as automatic shutdown, alarms).

- Control equipment including, but not limited to air conditioning and water detection.
- Prevention of water damage, location of water tanks, pipes etc. within the premises.

9.6 The 3rd Party must ensure that physical access to areas that are hosting BT Information is with smart or proximity cards (or equivalent or better security systems) and 3rd Party must conduct monthly checks to ensure only relevant individuals are provided with this access.

9.7 The 3rd Party must ensure that photography and/or the image capture of any BT Information is prohibited. Where there is a business need to capture such images, confirmation must be obtained in writing from the BT Stakeholder.

10. Provision of Hosting Environment for BT Equipment

10.1 The 3rd Party must, where the 3rd Party is providing a secure access area on their premises for hosting BT or BT customer equipment:

- Provide BT with a floor plan of allocated space in the secure area of the premises.
- Ensure that BT and BT customer cabinets at the premises are kept locked and only accessed by authorised BT personnel, BT approved representatives and relevant 3rd Party Personnel.
- Implement a secure key management process.

10.2 BT shall provide the 3rd Party with:

- A record of BT and/or BT customer's physical assets held at the 3rd Party premises.
- Details of BT's employees, subcontractors and agents that need access to the 3rd Party premises (on an on-going basis).

11. Secure Software Development

11.1 The 3rd Party must ensure that production and non-production environments are appropriately controlled by ensuring the following components are in place:

- Segregation of production and non-production environments with segregation of duty.
- No live data to be used in test unless prior agreement from the data owners and controls commensurate with the production environment.
- Segregation of duties between production and non-production development.

11.2 The 3rd Party must have an established and consistent Systems Development framework to prevent security vulnerabilities and Cyber Security breaches which contains the following components:

- Systems are developed in line with Secure Development best practice (e.g. OWASP).
- Code is securely stored and subject to Quality Assurance.
- Code is adequately protected from unauthorised modification once testing has been signed off and delivered into production.

12. Escrow

12.1 Where Escrow is required to protect all parties for either 1st party or 3rd Party Escrow (i.e. for Intellectual Property / Source code etc.) the 3rd Party must have a consistent and established framework which includes the following components:

- Execution of escrow agreement with independent, neutral, and reputable Escrow agent.
- Delivery and ongoing updates of source code and other materials to the Escrow agent to ensure the required information is up to date.
- Secure storage of source code and other materials until release conditions are met.
- Appropriate release conditions.
- Ongoing updates, appropriate payments, and reviews to the Escrow agreement.

13. Access to BT Systems

13.1 The 3rd Party shall adhere to all relevant instructions provided to them with regards to access and use of BT Systems.

13.2 3rd Party is responsible for advising BT with 24 hours when a 3rd Party individual no longer requires access.

13.3 The 3rd Party shall ensure user identification, passwords, PINs, tokens, and conferencing access are for individual 3rd Party Personnel and not shared. Details must be stored securely and separately from the device that is used to access. If a password is known by another person, it must be changed immediately.

System to System connectivity

13.4 Inter domain linking to BT Systems is not permissible unless specifically approved and authorised by BT.

13.5 The 3rd Party must use all reasonable endeavours to ensure no malware (as the expression is generally understood in the computing industry) is introduced to BT Systems.

13.6 Where there is connectivity between the 3rd Party and BT systems the connectivity will be via secure links with data protected by encryption conforming to the cryptography controls in 14.9, 14.10, 14.11, 14.12 and 14.13.

13.7 The 3rd Party will ensure that the systems and infrastructure used are contained within a dedicated logical network. This network must consist only of the systems dedicated to delivery of a secure customer data processing facility.

14. 3rd Party Systems holding BT Information

14.1 3rd Party must ensure that the latest security patches are applied to systems/assets/Networks/applications ensuring that:

- 3rd Party deploys patches as soon as reasonably practicable and uses best endeavours to deploy within the following timescales following patch release:

	Actively exploited in the wild	**High EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: >= 70% (Network Attack Vector – see definitions section)	**Lower EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: < 70% (Network Attack Vector – see definitions section)	**Other** (non-Network Attack Vector)
Externally exposed interface	7 days	14 days	30 days	90 days
Internally exposed interface	7 days	14 days	30 days	90 days/BAU

- 3rd Party uses patches obtained from: vendors directly for proprietary systems and patches that are either (i) digitally signed or (ii) verified via the use of a vendor hash (MD5 hashes must not be used) for the update package such that the patch can be identified as coming from a reputable support community for open-source software.
- 3rd Party tests all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity.
- Monitoring all applicable vendors and other relevant information sources for vulnerability alerts.
- If a system cannot be patched deploy appropriate countermeasures.
- 3rd Party will install critical security patches separately to feature releases to maximise the speed at which the patch can be deployed and will prioritise critical security patches over functionality upgrades wherever possible.

14.2 The 3rd Party must ensure that at least on an annual basis, an independent IT security assessment / penetration test approved by BT Security is commissioned on the 3rd Party IT infrastructure and applications used to provide services, including Disaster Recovery sites to identify vulnerabilities that could be exploited to breach data / services and to prevent against any security breaches through Cyber Attacks. The 3rd Party must on reasonable request permit BT access to penetration test reports relevant to the services being provided.

14.3 The 3rd Party must ensure that access to diagnostic and management ports as well as diagnostic tools are securely controlled.

14.4 The 3rd Party must ensure that access to audit tools is restricted to relevant supplier personnel and their use is monitored.

14.5 The 3rd Party must ensure that any servers used to provide the service are not deployed on untrusted networks (networks outside the 3rd Party security perimeter, that are

beyond its administrative control e.g. internet-facing) without appropriate security controls.

Asset Management

14.6 The 3rd Party must maintain an accurate and up-to-date information asset inventory of all technology assets with the potential to store or process information, so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access. This inventory shall include all hardware assets, whether connected to the organisation's network or not. If applicable, any BT equipment hosted in 3rd Party premises shall be included in the inventory.

14.7 The 3rd Party must ensure that the information asset inventory has the following components inventoried or catalogued:

- Physical devices and systems, software platforms and applications, external information systems.
- Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value.
- Organisational and Communication Data Flows including external / 3rd Party flows.
- Manual processes that handle BT or BT Customer data.

14.8 The 3rd Party must maintain an accurate and up-to-date software asset inventory for all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installing or executing.

Cryptography

14.9 The 3rd Party must ensure that BT Information classified as Confidential or higher, is appropriately encrypted (in transit and at rest). All encryptions shall be accomplished with strong, modern cryptographic algorithms and ciphers employing robust integrity protection mechanisms and in accordance with industry standards for secure key and protocol negotiation and key management. For data in transit the following TLS options are not allowed: TLS v1.0, TLS v1.1 and SSL (any version). The following SSH (SFTP) options are not allowed: SSH v1. The following IPSec options are not allowed: IKE Version 1.

14.10 Cryptographic keys must meet or exceed the following minimum lengths:

- Symmetric keys (e.g., AES) must have a key length of at least 256 bits.
- Asymmetric keys (e.g., RSA) must have a key length of at least 3072 bits.
- Elliptic Curve keys must have a key length of at least 384 bits.

14.11 If NIST announces a crypto algorithm is no longer secure, it must not be used for new deployments. Existing deployments must review the continued use of deprecated crypto algorithms and deliver a migration plan to move away from deprecated crypto algorithms to a more secure alternative.

14.12 For symmetric encryption the following algorithms are not allowed; 3DES-168 (unless mandated by an international standard), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed and ARIA.

14.13 Salted hashes must be used to protect data in storage i.e. passwords. Hashing may also be used to anonymise data before processing, for example MSISDNs or payment. The following hashing algorithms are not allowed MD2, MD4, MD5 and SHA-1.

System Configuration

14.14 The 3rd Party must have an established and consistent framework to ensure that systems are appropriately configured including the following components:

- Systems, network devices are configured to function in accordance with security principles (e.g., concept of least functionality and no unauthorised software).
- Ensuring that devices have the correct and consistent time.
- Systems are free from any malicious software.
- Appropriate checks and monitoring are in place to ensure the integrity of the builds / devices are maintained.

Malware protection

14.15 The 3rd Party must ensure that the most up to date malware protection is applied to all applicable IT assets to prevent service disruption or security breaches and ensure that appropriate user awareness procedures are implemented.

Anti-malware shall include detection for (but not limited to) ransomware, unauthorised mobile code, viruses, spyware, key logger software, botnets, worms, trojans etc.

Denial of Service Mitigations.

14.16 The 3rd Party must ensure that key systems are protected against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

15. 3rd Party Hosting BT Information

15.1 In addition to the controls in Section 14. 3rd Party Systems holding BT Information, where 3rd Party is hosting BT's Information in a datacentre or cloud solution the premises must hold a valid ISO/IEC 27001 certificate for security management (or certification(s) that demonstrate equivalent controls, supported by an independent auditor report).

16. Network Security – BT's own Network

Where 3rd Party will be installing equipment into, configuring, maintaining, managing, repairing, or monitoring BT's own network the following controls will apply:

16.1 Upon request, the 3rd Party shall provide BT with the names, addresses and such other details as BT shall reasonably require of all individual 3rd Party Personnel who:

- shall from time to time be directly involved in the deployment, maintenance and/or management of the Service(s) before they are respectively engaged.

- shall liaise with BT in relation to discussion around BT- and/or 3rd Party-identified vulnerabilities in the Service(s).

16.2 In relation to its UK-based support activities, the 3rd Party shall retain a skilled security team comprised of at least one UK national who shall be available for liaison with BT and the team shall attend such meetings as BT shall from time to time reasonably require.

16.3 The 3rd Party shall provide BT with a schedule (updated as necessary from time to time) of all active components comprised in the Service(s) and their respective sources.

16.4 The 3rd Party shall ensure that installation of new systems, equipment or software on BT's own network utilises the most recent software version and patch.

16.5 The 3rd Party shall ensure that all security-relevant logging is enabled on all network equipment installed by the 3rd Party and sent to the BT network logging systems.

16.6 The 3rd Party shall provide BT with timely (i.e., as soon as practicable to allow remediation before publicly publishing) information in relation to any vulnerabilities in the Service(s) and comply (at the 3rd Party's cost) with such reasonable requirements in relation to vulnerabilities as may be notified by BT.

16.7 The 3rd Party shall ensure that any security-related components comprised in the Service(s) as are identified by or to BT from time to time are, at the 3rd Party's cost, externally evaluated to BT's reasonable satisfaction.

16.8 The 3rd Party shall promptly, and in any event within 7 Working Days, provide to BT full details of any features and/or functionality in the Service(s) or that are planned in the Roadmap for the Service(s) that from time to time:

- the 3rd Party knows; or
- BT reasonably believes and so informs the 3rd Party are designed for, or could be used for, lawful interception or any other interception of telecommunication's traffic. Such details shall include all Information that is reasonably necessary to enable BT to fully understand the nature, composition, and extent of such features and/or functionality.

16.9 The 3rd Party must not use any network monitoring tools that can view application information.

16.10 The 3rd Party Personnel building, developing, and/or supporting BT's own network shall have as a minimum L2 pre-employment check. L3 pre-employment checks will be required for roles identified by BT.

16.11 3rd Party shall permit BT to install security software to BT's specification, on any 3rd Party virtual infrastructure (including but not limited to virtual machines and containers) or 3rd Party-installed operating system running on BT Networks.

16.12 3rd Party must ensure that the latest security patches are applied to systems/assets/Networks/applications ensuring that:

- 3rd Party deploys patches as soon as reasonably practicable and uses best endeavours to deploy within the following timescales following patch release:

	Actively exploited in the wild	**High EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: >= 70% (Network Attack Vector – see definitions section)	**Lower EPSS** Vulnerability CVSS: > 8.0 (High + Critical) EPSS: < 70% (Network Attack Vector – see definitions section)	**Other** (non-Network Attack Vector)
Externally exposed interface	7 days	14 days	30 days	90 days
Internally exposed interface	7 days	14 days	30 days	90 days/BAU

- 3rd Party uses patches obtained from: vendors directly for proprietary systems and patches that are either (i) digitally signed or (ii) verified via the use of a vendor hash (MD5 hashes must not be used) for the update package such that the patch can be identified as coming from a reputable support community for open-source software.
- 3rd Party tests all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity.
- Monitoring all applicable vendors and other relevant information sources for vulnerability alerts.
- If a system cannot be patched deploy appropriate countermeasures.
- 3rd Party will deliver critical security patches separately to feature releases to maximise the speed at which the patch can be deployed and will prioritise critical security patches over functionality upgrades wherever possible.

Telecommunications (Security) Act 2021 (TSA)

Where the 3rd Party is supplying or making available goods, services or facilities for use in connection with a UK public electronic communications network or service, the following security controls apply.

16.13 Where 3rd Party is supporting more than one operator, controls must be implemented to prevent one operator or their network from adversely affecting any other operator or their network.

16.14 Where 3rd Party is operating as a 3rd Party Administrator for more than one operator, the following controls apply:

- Implement logical separation within the 3rd Party network to segregate customer data and networks.
- Implement separation between 3rd Party management environments used for different operator networks.

- Implement and enforce security enforcing functions at the boundary between the 3rd Party network and the operator network.
- Implement technical controls to limit the potential for users or systems to negatively impact more than one operator.
- Implement physically and logically independent Privileged Access Workstations per operator.
- Implement independent administrative domains and accounts per operator.

16.15 When providing network equipment 3rd Parties must provide BT with a 'security declaration' on how secure equipment is produced and how the equipment's security is ensured throughout its lifetime. This security declaration shall cover the requirements of the Vendor Security Assessment published at Annex B of the Telecommunications Security Code of Practice, and shall be approved at an appropriate level of seniority agreed with BT.

16.16 Where the 3rd Party is providing network equipment the following controls are applicable:

- 3rd Party warrants that it will adhere to a standard no lower than its published 'security declaration'.
- 3rd Party will supply up-to-date guidance on how the equipment should be securely deployed.
- 3rd Party will support all equipment and all software and hardware subcomponents for the length of the contract.
- 3rd Party will provide details for all major 3rd party components and dependencies, including but not restricted to, product and version, open-source components and level of support and period.
- 3rd Party will remediate all security issues that pose a security risk to BT's network or service discovered within their products within a reasonable time of being notified, providing regular updates on progress in the interim – such time to be agreed between BT and the 3rd Party both acting reasonably. This shall include all products impacted by the vulnerability, not only the product for which the vulnerability was reported.
- 3rd Party will either remove or change default passwords and default or hardcoded accounts or ensure that the network equipment is configured to enable BT to do so.
- 3rd Party will wherever possible disable unencrypted management protocols, and where not possible identify the presence of such protocols to BT to enable their use to be mitigated.

16.17 If 3rd Party has obtained internationally recognised security assessments or certifications for equipment (e.g., Common Criteria or NESAS), they shall share with BT the full findings that evidence this assessment or certificate.

16.18 Where 3rd Party's own network has potential to impact BT's Networks, the 3rd Party will, as advised by BT, undergo the same level of testing as BT applies to BT's Networks and will remediate identified vulnerabilities as agreed by both parties.

16.19 3rd Party authorises BT to share details of security issues as appropriate where necessary for the purposes of network security.

16.20 Infrastructure and Systems used to maintain BT's Networks must be located within the UK.

16.21 Where 3rd Party is performing BT's Network Oversight Functions, equipment used for this function shall be both located within the UK and operated using UK-based staff.

16.22 Where 3rd Party is responsible for network security and audit logs, these shall be stored within the UK and protected subject to UK law.

16.23 Where 3rd Party is operating as a 3rd Party Administrator, BT retains the right to determine permissions of the accounts used by the 3rd Party to access its network, and to require all logs relating to the security of the 3rd Party network to the extent that such logs relate to access into BT's network. The 3rd Party shall monitor and audit the activities of its staff when accessing BT's network.

17. 3rd Party Network Security

17.1 The 3rd Party must ensure that network integrity is established and maintained by ensuring the following components are appropriately controlled, and notifying BT in any instances where this is not technically possible:

- External connections to the network are documented, routed through a firewall and verified and approved prior to the connections being established to prevent data security breaches.
- The network is appropriately designed using "defence in depth" principles to ensure Cyber security breaches are minimised by ensuring appropriate controls that prevent any purposeful attack, such as "network segmentation", are in place.
- The design and implementation of the network is reviewed at least annually.
- All wireless access to the network is subject to authorisation, authentication, segmentation, and encryption protocols to prevent security breaches.
- Using secure communications between devices and management stations.
- Using secure communications between devices as appropriate; including the encryption of all non-console administrator access.
- Using strong architectural design, which are tiered and zoned with effective identity management and operating system configuration which must be appropriately hardened and documented.
- By the disabling (where practical) of services, applications and ports that will not be used.
- By the disabling or removal of guest accounts.
- By the avoidance of trust relationships between servers.
- Use of the best practice security principle of "least privilege" to perform a function.
- Ensuring appropriate measures are in place for intrusion detection and/or protection.
- Where appropriate, file integrity monitoring to detect any additions, modifications or deletions of critical system files or data.

- Change all default and vendor supplied passwords before network components go live.
- Disable unencrypted management protocols wherever technically possible.

17.2 The 3rd Party Network shall meet all legal and regulatory requirements, and:

- Use best endeavours to prevent unauthorised individuals (e.g. hackers) from gaining access to the 3rd Party Network(s).
- Use best endeavours to reduce the risk of misuse of the 3rd Party Network(s) by those individuals authorised to access it.
- Use best endeavours to detect any Security Breaches and ensure quick rectification of any breaches, alongside the identification of the individuals who obtained access and determination of how they obtained it.

Telecommunications (Security) Act 2021

17.3 Where the 3rd Party is supplying or making available goods, services or facilities for use in connection with a UK public electronic communications network or service, the following additional security controls apply:

- Externally facing systems, excluding Customer Premises Equipment (CPE), are security tested every two years or when there is a significant change.
- Sensitive datasets and sensitive or critical functions are not hosted on equipment at the Exposed Edge of the network.
- If not cryptographically protected, physical and logical separation shall be implemented between the Exposed Edge and sensitive or critical functions.
- Security separation using security enforcing functions shall be implemented between the Exposed Edge and sensitive or critical functions.

18. Cloud Security

18.1 The 3rd Party must be certified to the latest version of ISO27017 or have an established and consistent framework to ensure that all use of Cloud technology and non-public data stored in the Cloud is approved and subject to appropriate controls equivalent to the latest version of the Cloud Security Alliance, Cloud Controls Matrix (CCM).

18.2 Network and infrastructure service level agreements (in-house or outsourced) shall clearly document shared responsibilities, security controls, capacity and service levels, and business or customer requirements.

18.3 3rd Party must implement security measures across all aspects of the service being supplied, such that it safeguards the confidentiality, availability, quality, and integrity by minimizing the opportunity of unauthorised individuals (e.g., other cloud customers) from gaining access to BT Information and the services utilised by BT.

18.4 To the extent 3rd Party provides hosted applications or services to BT, whether single-tenant or multi-tenant, including software-as-a-service, platform-as-a-service, infrastructure-as-a-service, and similar offerings, to collect, transmit, store, or otherwise process Confidential Data, 3rd Party shall provide BT the ability:

- to isolate such Confidential Data logically from the data of 3rd Party's other customers.

- to restrict, log, and monitor access to such Confidential Data at any time including access by 3rd Party Personnel
- to create, enable, disable, and delete the uppermost encryption key (known as Customer Managed Key) used to encrypt and decrypt subsequent keys including the lowermost data encryption key.
- to restrict, log, and monitor access to the Customer Managed Key at any time; and at no time shall any subsequent encryption key, an encryption key in a key hierarchy lower than the Customer Managed Key, be stored in the same system as Confidential Data unless encrypted by the Customer Managed Key, also known as being wrapped by the Customer Managed Key.

19. SIM Cards

19.1 Where the 3rd Party is providing SIM Cards, the following controls are applicable:

- For fixed-profile SIM cards, 3rd Party shall ensure that sensitive SIM data is appropriately protected by the SIM card manufacturer.
- For fixed-profile SIM cards, 3rd Party shall ensure that, the confidentiality integrity and availability of the sensitive SIM card data shared with the SIM card manufacturer is protected at every stage of their lifecycle.

20. Information classified as OFFICIAL or higher by HMG

20.1 The additional Security Requirements set out in Annex 1 to these Security Requirements will apply to each 3rd Party that will store, process or transmit information classified as OFFICIAL in line with His Majesty's Government Security Classifications Scheme as updated from time to time.

21. Defined Terms and Interpretation

21.1 Unless otherwise defined below, words and expressions used in these Security Requirements will have the same meaning as in the Contract:

"**Access**" and **"Accessed"** means the Processing, handling or storing BT Information by one or more of the following methods:

a. by interconnection with BT Systems;

b. provided in paper or non-electronic format;

c. BT Information on Supplier Systems; or

d. by mobile media

and/or Access to BT premises for the provision of the Supplies excluding the delivery of hardware and meeting attendance.

"**BT Information**" means all Information relating to BT or a BT Customer provided to the Supplier and all Information which is processed or handled by the Supplier on behalf BT or a BT Customer under the Contract.

"BT Stakeholder" means the BT representative who has ownership of the scope of work 3rd Party is undertaking.

"**BT Systems**" means the Services and Service components, products, networks, servers, processes, paper-based system or IT systems (in whole or part) owned and/or operated by BT or such other systems that may be hosted on BT premises.

"BT's Networks" means any Public Electronic Communications Network operated by BT, as defined by section 32 of the Communications Act 2003.

"BYOD" means bring your own device.

"**Contract**" means the Contract entered into by the Parties for the supply of goods, software or Services which references these Security Requirements.

"Customer Premises Equipment" means equipment provided to customers by the provider, and managed by the provider, that is used, or intended to be used, as part of the network or service. This excludes consumer electronic devices such as mobile phones and tablets, but does include devices such as edge firewalls, SD-WAN equipment, and fixed wireless access kit. ""

"**Cyber Essentials Plus**" means UK Government backed scheme to help organisations protect themselves against common cyber-attacks.

"Cyber Security" means how individuals and organisations reduce the risk of cyber-attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage.

"EPSS" means the Exploit Prediction Scoring System.

"**Escrow**" means the source code deposit agreement entered into in accordance with the Contract, to use, copy, maintain and modify such source code for the business purposes of BT (including the right to compile such source code).

"**Exposed Edge**" means Equipment that is either within customer premises, directly addressable from customer/user equipment, or is physically vulnerable. Physically vulnerable equipment includes equipment in road-side cabinets or attached to street furniture. The Exposed Edge includes CPEs, base station equipment, OLT equipment and MSAN/DSLAM equipment.

"**Good Industry Security Practice**" means in relation to any undertaking and any circumstances, the implementation of the security practices, policies, standards and tooling which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances.

"NDA" means a non-disclosure agreement is a binding contract between two or more parties that prevents sensitive information from being shared with others.

"NESAS" means the GSM Association's Network Equipment Security Assurance Scheme.

"Network Asset" means an item that is part of a collection of interconnected components such as computers, routers, hubs, cabling, and telecommunications controllers that make up a network.

"Network Attack Vector" means that the vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options listed below, up to and including the entire Internet. Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable at the protocol level one or more network hops away (e.g., across one or more routers). An example of a

network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet across a wide area network (e.g., CVE 2004 0230).

"Network Oversight Function" means the components of BT's Network that oversee and control the security critical functions, which make them vitally important in overall network security. They are essential for BT to understand the network, secure the network, or to recover the network.

"**Network Security**" means the security of the interconnecting communication paths and nodes that logically connect end user technologies together and associated management systems.

"NIST" means The National Institute of Standards and Technology - a unit of the U.S. Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

"**Official Sensitive Declaration**" means the written declaration to be provided by the Supplier relating to roles identified by the Supplier as having Access to information classified as "Official Sensitive" or having elevated privileges to infrastructure that stores, processes or transmits information classified as "Official Sensitive", a template of which is set out in Annex 1.

"Privileged Access Workstation (PAW)" means workstations through which Privileged Access is possible.

"Security Critical Function" means any function of BT's Network or the Service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it.

"**Security Requirements**" means this document as updated from time to time.

"SIM" means a unique hardware component or token, and associated software, used to authenticate the subscriber's access to the network. As used in this document, the SIM encompasses the hardware UICC/eUICC, the SIM/USIM/ISIM applications, eSIM and RSP functionality and any SIM applets.

"**Subcontractor**" means a Subcontractor of the Supplier which performs or is involved in the provision of the Supplies, or which employs or engages persons engaged in the provision of the Supplies.

"**Service**" means any and all of the "**Goods**", "**Software**" or "**Services**" as defined in the Contract.

"Transaction" means transactional data/ information that is captured from transactions i.e., data generated by various applications while running or supporting everyday business processes.

"Trusted Platform Module" means technology designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM. The most common TPM functions are used for system integrity measurements and for key creation and use. During the boot process of a system, the boot code that is loaded (including firmware and the operating system components) can be measured and recorded in the TPM. The integrity measurements

can be used as evidence for how a system started and to make sure that a TPM-based key was used only when the correct software was used to boot the system.

"3rd Party" means a Supplier to BT.

"3rd Party Administrator" means a managed service provider, provider of group functions, or external support for third party supplier equipment (e.g. third-line support function)

"**3rd Party Personnel**" means any persons engaged by the Supplier or its Subcontractors in the performance of the Supplier's obligations under the Contract.

"3rd Party Network" means any Supplier network.

"**3rd Party System**" means any Supplier owned computer, application or network systems used for accessing, storing or processing BT Information or involved in the provision of the Supplies.

Interpretation

21.2 Any words following the terms "including", "include", "in particular", "for example" or any similar expression will be construed as illustrative and will not limit the sense of the words, description, definition, phrase or term preceding those terms.

21.3 Any time a Party's right or obligation is expressed as one that they "**may**" exercise or perform, the option to exercise or perform that right or obligation will be in that Party's sole discretion.

21.4 Where any hyperlink ("**URL**") is referenced, such reference will be to such online resource Accessible via that URL, or such other replacement URL as notified to the applicable Party from time to time.

Version	Description	Author	Date
5.0	Telecommunications (Security) Act 2021 (TSA) Legislation and BT's adoption of CIS	Jemma Turner	25/10/22
5.1	Amendment to 14.9 TLS	Jemma Turner	17/04/23
5.2	Alterations to various clauses to incorporate TSA and vulnerabilities	Jemma Turner	30/11/23

ANNEX 1 – Additional Security Requirements

Where the 3rd Party is required to Access, store, process or transmit information classified as OFFICIAL or above, the 3rd Party will comply with the BT Security Requirements and additionally the requirements set out in this Annex 1. In all cases, the highest-level control will supersede requirements documented elsewhere in these Security Requirements.

1. EMPLOYEES

1.1 All 3rd Party Personnel employed having access to information classified as OFFICIAL or above or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL or above:

1.1.1 must be subject to pre-employment screening to Baseline Personnel Security Standard (BPSS) standard as a minimum;

1.1.2 must sign an Official Secrets Act declaration; and

1.1.3. must be prevented from accessing information or systems unless they have the required security clearances as specified in the relevant contract.

2. SECURITY TRAINING

2.1. The 3rd Party will mandate security training upon hire and at least annually for all employees having access to information classified as OFFICIAL or above or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL or above. This training shall cover the information handling requirements in line with the requirements of His Majesty's Government Security Classifications Scheme, as detailed in BT's Protecting HMG Information Guidance for 3rd Parties which shall be provided to the 3rd Party by BT.

2.2. The 3rd Party will update job descriptions for all employees having access to information classified as OFFICIAL or above or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL or above, to mandate participation in training described in paragraph 2.1 above. The 3rd Party will maintain a record of training which must be made available to BT upon request.

3. ACCESS CONTROL

3.1. When employees leave or move roles, their access rights must be revoked from relevant 3rd Party Systems within 1 Business Day.

3.2. Where the 3rd Party's employees, including contractors, temporary employees and agency workers, have elevated privileges to the BT infrastructure, the 3rd Party must notify BT in writing within 1 Business Day from when an employee no longer requires Access to BT Systems (e.g. employees leave or move roles).

3.3. Where the 3rd Party's employees, including contractors, temporary employees and agency workers, are issued with permanent Access cards to BT premises, the 3rd Party must notify BT in writing within 1 Business Day when an employee no longer requires Access to BT premises (e.g. employees leave or move roles).

4. VALUATION AND CLASSIFICATION OF ASSETS

4.1. The 3rd Party will implement additional information handling procedures to meet handling requirements in line with the requirements of His Majesty's Government Security Classification Scheme as updated from time to time.

5. INCIDENT RESPONSE AND REPORTING – SERVICE LEVEL AGREEMENTS

5.1. The 3rd Party will be advised on specific Service level agreements to support the incident response process. These may supersede any previous agreement outlined in these Security Requirements.

6. AUDIT, TESTING AND MONITORING

6.1. The 3rd Party will implement 24/7 security monitoring where specified by BT for the 3rd Party's infrastructure that supports the processing, storage or transmission of information classified as OFFICIAL or above.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY

7.1. The 3rd Party will produce a business continuity and disaster recovery plan in accordance with BS ISO 22301 within 30 days of contract signature.

8. LOCATION

8.1. Unless specified otherwise by BT, the Service must be physically located within the physical boundaries of the UK or, if applicable, the EEA. Any remote support and/or management of the Service by the Supplier from an offshore location shall only be performed in accordance with the approvals process set out in the applicable contract between BT and the Government department concerned.

9. ADDITIONAL REQUIREMENTS FOR OFFICIAL-SENSITIVE OR ABOVE

9.1 All roles identified by the 3rd Party as having Access to information classified as OFFICIAL-SENSITIVE or above, or having elevated privileges to infrastructure that stores, processes or transmits information classified as OFFICIAL-SENSITIVE or above shall be documented in the OFFICIAL-SENSITIVE Declaration and provide BT with the completed OFFICIAL-SENSITIVE Declaration prior to Contract signature.

9.2 Where the Supplier is required to access, store, process or transmit information classified as HMG OFFICIAL-SENSITIVE or higher the Supplier to conduct a Personnel Security Risk Assessment on all roles identified in the OFFICIAL-SENSITIVE Declaration para 2 in line with the requirements set out in the document National Protective Security Authority (NPSA) Personnel Security Risk assessment - A guide (4th Edition - June 2013 or later).

ANNEX 1, EXHIBIT 1 – OFFICIAL SENSITIVE DECLARATION TEMPLATE

1. Systems/Services in Scope

Please list the systems and Services being provided in support of the HMG customer.

System	Service

2. 3rd Party roles requiring a security clearance level.

Role	Required Security Clearance Level
* e.g. DBA	SC

3. Vulnerability Management

System	Type of vulnerability Assessment	Frequency

4. Audit, Testing and Monitoring

Systems to be monitored 24/7 as advised by BT

ANNEX 2, Telecommunications (Security) Act 2021 - Code of Practice to Security Requirements conversion

Code Numbering	Requirement	BT Security Requirement Clause
M1.02	Security testing on externally facing systems, excluding CPE, should normally be performed at least every two years, and in any case shortly after a significant change occurs.	17.3
M1.03	Equipment in the exposed edge shall not host sensitive data or security critical functions.	17.3
M1.04	Physical and logical separation shall be implemented between the exposed edge and security critical functions. Note that this measure may not be necessary once datasets and functions can be cryptographically protected from compromise	17.3
M1.05	Security boundaries shall exist between the exposed edge and critical or sensitive functions which implement protective measures.	17.3
M2.02	All privileged access shall be logged.	3.56, 3.57
M2.06	The infrastructure used to support a provider's network shall be the responsibility of the provider, or another entity that adheres to the regulations, measures and oversight as they apply to the provider (such as a third-party supplier with whom the provider has a contractual relationship). Where the provider or other entity adhering to the regulations has responsibility, this responsibility shall include retaining oversight of the management of that infrastructure (including sight of management activities, personnel granted management access, and management processes).	3.56, 3.57 and 4, 14
M5.05	Providers shall perform a root-cause analysis of all security incidents. Outcomes of this analysis shall be escalated to an appropriate level, which may include the provider's board.	3.36
M6.01	Non-persistent credentials (e.g. username and password authentication) shall be stored in a centralised service with appropriate role-based access control which shall be updated in line with any relevant changes to roles and responsibilities within the organisation.	3.44
M6.02	Privileged access shall be via accounts with unique user ID and authentication credentials for each user and these shall not be shared.	3.47
M6.04	All break-glass privileged user accounts must have unique, strong credentials per individual piece of network equipment.	3.48
M6.05	Default and hardcoded accounts shall be disabled.	16.16

M8.05	Providers shall record all equipment deployed in their networks, and proactively assess, at least once a year, their exposure should the third-party supplier be unable to continue to support that equipment.	16.16, 16.5
M8.06	Providers shall remove or change default passwords and accounts for all devices in the network and should disable unencrypted management protocols. Where unencrypted management protocols cannot be disabled, providers shall limit and mitigate the use of these protocols as far as possible.	16.16 and 17.1
M8.07	Providers shall ensure that all security-relevant logging is enabled on all network equipment and sent to the network logging systems.	16.5
M8.08	Providers shall prioritise critical security patches over functionality upgrades wherever possible.	14.1 and 16.12
M8.12	For fixed-profile SIM cards, the provider shall ensure that sensitive SIM data is appropriately protected throughout its lifecycle, by both the SIM card vendor and within the operator network, given the risk to network resilience and confidentiality should this information be lost.	19.1
M8.13	For fixed-profile SIM cards, the confidentiality, integrity and availability of the sensitive SIM card data shared with the SIM card vendor shall be protected at every stage of their lifecycle.	19.1
M10.04	The provider's incident management process and that of their third-party suppliers shall provide mutual support in the resolution of incidents.	3.31-3.36
M10.06	The provider shall define what information is made accessible to any third-party supplier, ensuring that it is the minimum necessary to fulfil their function. Providers shall place controls on that information and limit third party access to the minimum required to fulfil the business function.	3.44
M10.09	Where network or user data leaves a provider's control, the provider shall contractually require and verify that the data is properly protected as a consequence. This shall include assessing the third-party supplier's controls to ensure provider data is only visible or accessible to appropriate employees and from appropriate locations.	3.44-3.50 and 14, 15, 17 and 18
M10.11	Providers shall contractually oblige third party suppliers to notify the provider within 48 hours of becoming aware of any security incidents that may have caused or contributed to the occurrence of a security compromise, or where they identify an increased risk of such a compromise occurring. This includes, but is not limited to, incidents in the supplier's development network or their corporate network.	3.33

M10.12	Providers shall contractually require third party suppliers to support the provider in investigations of incidents that cause or contribute to the occurrence of a security compromise in relation to the primary provider, or of an increased risk of such a compromise occurring.	3.31-3.36
M10.13	Providers shall contractually require the third-party suppliers to find and report on the root cause of any security incident that could result in a security compromise in the UK within 30 days and rectify any security failings found.	3.35
M10.16	Providers shall contractually require third party suppliers to support, as far as appropriate, any security audits, assessments or testing required by the provider in relation to the security of the provider's own network, including those necessary to evaluate the security requirements in this document.	5.1-5.2, 6.1-6.3
M10.18	The provider shall retain the right to determine permissions of the accounts used to access its network by third party administrators.	16.23
M10.21	Providers shall have the contractual right to control the members of third-party administrator personnel who are involved in the provision of the third-party administrator services, including to require the third-party administrator to ensure that any member of personnel no longer has access to the network.	13.1
M10.24	Providers shall contractually require that the third-party administrators implement technical controls to prevent one provider or their network from adversely affecting any other provider or their network.	16.13
M10.25	Providers shall contractually require that the third-party administrators implement logical separation within the third-party administrator network to segregate customer data and networks.	16.14
M10.26	Providers shall contractually require that the third-party administrators implement separation between third party administrator management environments used for different provider networks.	16.14
M10.27	Providers shall contractually require that the third-party administrators implement and enforce security enforcing functions at the boundary between the third-party administrator network and the provider network.	16.14
M10.28	Providers shall contractually require that the third-party administrators implement technical controls to limit the potential for users or systems to negatively impact more than one provider.	16.14

M10.29	Providers shall contractually require that third party administrators implement logically independent privileged access workstations per provider.	16.14
M10.30	Providers shall contractually require that third party administrators implement independent administrative domains and accounts per provider.	16.14
M10.33	The provider shall contractually require the third-party administrator to monitor and audit the activities of the third-party administrator's staff when accessing the provider's network.	3.56, 3.57
M10.34	The provider shall contractually require from the third-party administrator all logs relating to the security of the third-party administrator's network to the extent that such logs relate to access into the provider's network.	3.56, 3.57 and 16.23
M10.35	Providers shall require that networks of the third-party administrator that could impact the provider undergo the same level of testing as the provider applies to themselves (e.g. TBEST testing as set for the provider by Ofcom from time to time).	16.18
M10.36	Providers shall contractually require network equipment suppliers to share with them a 'security declaration' on how they produce secure equipment and ensure they maintain the equipment's security throughout its lifetime. It is recommended that any such declaration should cover all aspects described within the Vendor Security Assessment (VSA) (see Annex B), and providers should encourage their suppliers to publish a response to the VSA.	16.15
M10.38	Providers shall ensure, by contractual arrangements, that the network equipment supplier's security declaration is signed-off at an appropriate governance level.	16.15
M10.39	Where the network equipment supplier claims to have obtained any internationally recognised security assessments or certifications of their equipment (such as Common Criteria or NESAS), providers shall contractually require equipment suppliers to share with them the full findings that evidence this assessment or certificate.	16.17
M10.40	Providers shall contractually require network equipment suppliers to adhere to a standard no lower than the network equipment supplier's security declaration.	16.16
M10.41	Providers shall contractually require network equipment suppliers to supply up-to-date guidance on how the equipment should be securely deployed.	16.16
M10.42	Providers shall contractually require network equipment suppliers to support all equipment and all software and hardware subcomponents for the length of the contract. The	16.16

	period of support of both hardware and software shall be written into the contract.	
M10.43	Providers shall contractually require network equipment suppliers to provide details (product and version) of major third-party components and dependencies, including open-source components and the period and level of support.	16.16
M10.44	Where relevant to a provider's particular usage of equipment, providers shall contractually require third party suppliers to remediate all security issues that pose a security risk to a provider's network or service discovered within their products within a reasonable time of being notified, providing regular updates on progress in the interim. This shall include all products impacted by the vulnerability, not only the product for which the vulnerability was reported.	16.16
M10.46	Providers shall ensure that their contracts allow details of security issues to be shared as appropriate to support the identification and reduction of the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service as a result of things done or omitted by third party suppliers.	3.33 and 16.19
M10.47	Providers shall contractually require network equipment suppliers to deliver critical security patches separately to feature releases, to maximise the speed at which the patch can be deployed.	14.1 and 16.12
M11.02	Any persistent credentials and secrets (e.g., for break glass access) shall be protected and not available to anyone except for the responsible person(s) in an emergency.	3.44
M11.03	Central storage for persistent credentials shall be protected by hardware means. For example, on a physical host the drive could be encrypted with the use of a TPM. Where a virtual machine (VM) is used to provide a central storage service, that VM and the data included in it shall also be encrypted, use secure boot and be configured to ensure that it can only be booted within an appropriate environment. This is to ensure that data cannot be removed from the operational environment and accessed.	3.45
M16.12	Logs for network equipment in security critical functions shall be fully recorded and made available for audit for 13 months.	3.56, 3.57
M16.21	Indications of potential anomalous activity shall be promptly assessed, investigated and addressed	3.56, 3.57
M21.02	The measures to be taken by the provider under Regulation 3(3)(f) should normally include ensuring, so far as is reasonably practicable, that the equipment performing provider's network oversight functions is located within the UK and operated using UK-based staff.	16.21

M21.03	The provider shall retain a UK-based technical capability to provide subject matter expertise on the operation of the provider's UK networks and the risks to the provider's UK networks.	16.2, 16.20-16.22
M21.04	Where data is stored offshore, the provider shall maintain a list of locations where the data is held. The risk due to holding the data in these locations, including any risk associated with local data protection law, shall be managed as part of the provider's risk management processes.	3.8